Listing of Claims

1 – 7. (Cancelled)

8. (Currently Amended) A method ~~according to Claim 1, further comprising the steps of:~~ of controlling access to digital data in a file comprising:

obtaining a passphrase from a user;

generating a personal key based on the obtained passphrase;

generating a file encryption key;

encrypting the digital data in the file with the file encryption key to provide an encrypted file;

encrypting the file encryption key with the personal key to provide an encrypted file encryption key;

creating a file header containing the encrypted file encryption key;

associating the file header with the encrypted file;

obtaining a user identification associated with an owner of the file;

obtaining a file identification associated with the file; and

wherein the step of generating a personal key based on the obtained passphrase comprises the step of hashing the user identification, the passphrase and the file identification to provide the personal key.

9. (Original) A method according to Claim 8, further comprising the step of storing the file and the associated file header at a file server.

10. (Original) A method according to Claim 9, wherein the step of storing the file and the associated file header at a file server comprises the step of selectively storing the file and the file header based on a type of store requested by the user and an evaluation of whether an existing file and file header having the user identification and file identification are stored at the file server.

11-35. (Cancelled)

36. (Currently Amended) A system ~~according to Claim 29, further comprising:~~ for controlling access to digital data in a file comprising:

means for obtaining a passphrase from a user;

means for generating a personal key based on the obtained passphrase;

means for generating a file encryption key;

means for encrypting the digital data in the file with the file encryption key to provide an encrypted file;

means for encrypting the file encryption key with the personal key to provide an encrypted file encryption key;

means for creating a file header containing the encrypted file encryption key;

means for associating the file header with the encrypted file;

means for obtaining a user identification associated with an owner of the file;

means for obtaining a file identification associated with the file; and

wherein the means for generating a personal key based on the obtained passphrase comprises means for hashing the user identification, the passphrase and the file identification to provide the personal key.

37. (Original) A system according to Claim 36, further comprising means for storing the file and the associated file header at a file server.

38. (Original) A system according to Claim 37, wherein the means for storing the file and the associated file header at a file server comprises means for selectively storing the file and the file header based on a type of store requested by the user and an evaluation of whether an existing file and file header having the user identification and file identification are stored at the file server.

39-63. (Cancelled)

64. (Currently Amended) A computer program product ~~according to Claim 57, further comprising:~~ for controlling access to digital data in a file comprising:

a computer readable storage medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which obtains a passphrase from a user;

computer readable program code which generates a personal key based on the obtained passphrase;

computer readable program code which generates a file encryption key;

computer readable program code which encrypts the digital data in the file with the file encryption key to provide an encrypted file;

computer readable program code which encrypts the file encryption key with the personal key to provide an encrypted file encryption key;

computer readable program code which creates a file header containing the encrypted file encryption key; and

computer readable program code which associates the file header with the encrypted file;

computer readable program code which obtains a user identification associated with an owner of the file;

computer readable program code which obtains a file identification associated with the file; and

wherein the computer readable program code which generates a personal key based on the obtained passphrase comprises computer readable program code which hashes the user identification, the passphrase and the file identification to provide the personal key.

65. (Original) A computer program product according to Claim 64, further comprising computer readable program code which stores the file and the associated file header at a file server.

66. (Original) A computer program product according to Claim 65, wherein the computer readable program code which stores the file and the associated file header at a file server comprises computer readable program code which selectively stores the file and the file header based on a type of store requested by the user and an evaluation of whether an existing file and file header having the user identification and file identification are stored at the file server.

67-84. (Cancelled)